TL

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/991,057	11/21/2001	James D. Lyle	SII-800 [SIMG0103]	3778

60974 7590 11/01/2006

GIRARD & EQUITZ LLP
400 MONTGOMERY STREET
SUITE 1110
SAN FRANCISCO, CA 94104

EXAMINER	
POLTORAK, PIOTR	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 11/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/991,057	**Applicant(s)** LYLE, JAMES D.	
	Examiner Peter Poltorak	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 July 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2,5-9,13,14,17,20,22,25-30,32-34,54,56,71,72,75-77 and 79-104* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2,5-9,13,14,17,20,22,25-30,32-34,54,56,71,72,75-77 and 79-104* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The Amendment, and remarks therein, received on 27/17/06 have been entered and carefully considered.
2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior office action.

Response to Amendment

3. Applicant's arguments have been carefully considered.
4. As per 35 USC § 112 rejection directed towards the phrase "TMDS-like" link applicant contends the rejection and argues that not only the specification disclose that "TMDS-like" link is a link having some but not all of the characteristics of a TMDS link and also suggests that examples of TMDS-like links are provided. The arguments have been carefully considered and found persuasive. Although applicant's definition seems to be broad ("link having *some* but not all of the characteristics of a TMDS link") it is not indefinite. As a result the rejection is withdrawn.
5. As per claims 74 and 82 applicant clarifies the term the "key material" and the 35 USC § 112 rejection directed towards the term is withdrawn.
6. As per claims 2, applicant argues that the art of record does not teach claim 2 limitations. The examiner carefully considered applicant's argument and find them persuasive. As a result the art rejection directed towards claim 2 is withdrawn. As per claims 99, 100 or 80 applicant argues that Menezes fails to teach a challenge-response procedure.

In particular applicant argues that there is no suggestion that a receiver "A" should encrypt any "first data" (e.g. encrypt random number rB to generate an authentication message or that that such a transmitter should perform a predetermined mathematical function on such an authentication message to generate a result and then send an encrypted result to the sender.

The examiner carefully considered applicant's argument but found them non persuasive.

The examiner points to Menezes' 10.16 Remark section ("3. mutual authentication , using random number", pg. 402), wherein Receiver A sends an encrypted random number rA. The transmitter B performs a predetermined mathematical function (decrypting rA using its key Ek) that results in obtaining unencrypted rA. The transmitter B encrypts the result rA and sends it back to the receiver.

7. As per claim 88 applicant argues that Pfleeger does not disclose generation of translated data by processing the decrypted data and that the encrypting the translated data results in generating of re-encrypted data.

   The examiner points out that the argued limitations are not present in claim 88.

8. Also, applicant argues that Pfleeger does not disclose "intermediate host" configured to generate "first data" from second encrypted data (received from an original content source) including by decrypting the second encrypted data using a second secret value and to generate encrypted data (for transmission to a third device) by encrypting the first data using another secret value.

The examiner points out in secure communication channel between two computer devices that involves the process of encryption of transmitted data and decryption of received data as disclosed by Pfleeger, encryption and decryption process inherently uses secret values (keys). Pfleeger also discloses the need for an external party to communicate (distribute) encryption/decryption keys to two communicating entities (e.g. paragraph 36-37, below) and discusses that utilizing a chain of computing devices to communicate data from an origin to a destination (e.g. paragraph 33-35). Delivering data from an origin to a destination utilizing several computing devices wherein data transfer between a sender and a receiver (along the path from the origin to the destination) is encrypted (by a sender) and decrypted (by a receiver), and wherein an external agent distributes encryption/decryption key pairs to communicating senders/receivers results in at least some of the receivers to decrypt data with one key (a secret value, e.g.) and re-encrypting with another (secret value).

9. The newly introduced limitations argued by applicant in the remaining pages are addressed in this Office Action.

10. Claims 2, 5-9, 13-14, 17, 20, 22, 25-30, 32-34, 54, 56, 71-72, 75-77 and 79-104 have been examined.

Claim Objections

11. Claim 88 recites that "an external agent is configured to be coupled to the receiver and the receiver, wherein the receiver is configured ...". The limitation is not

understood. In light of a following limitation that recites that "the external agent is configured to respond to a ticket request from one of the repeater and the receiver" the claim limitations is treated as though the external agent is coupled to the receiver and the repeater. However, the appropriate amendment to claim 88 is required.

12. The phrase "to be coupled to be serial link" in claim 88 is treated as "to be coupled to the serial link".

13. Claim 90 recites a system comprising an external agent that in response to ticket requests sends signals to a transmitter, a receiver and a router. The claim language further specifies that the signals can include: data enabling the receiver to obtain the secret value, data enabling the router to obtain the second secret value, and data enabling the receiver to obtain the third secret value. Applicant is advised to verify that one of the underlined "receiver" should not read "transmitter".

14.

Claim Rejections - 35 USC § 112

15. Claims 2, 5-9, 13-14, 17, 20, 22, 25-30, 32-34, 54, 56, 71-72, 75-77 and 88-104 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention.

16. The structures of claims 2, 9 and 88-104 are ambiguous forcing a reader to guess required limitations. For example, claim 92 is directed towards a repeater. However, claim 92 extensively recites limitations directed towards a system comprising a repeater, a transmitter, a receiver and an external agent. From the

claim limitations it appears that the repeater can only be a part of an external agent but the relationship between the repeater and other system elements is not understood. Furthermore, the repeater is to be configured to implement content protections protocols (a content protection protocol and a second content protection protocol). Additionally, claim 92 puts additional restrictions on the content protections protocol; it recites that the external agent is "configured to perform at least one function essential to implementation" of the content protection protocols but does not disclose any of the essential functions.

17. The ambiguous relationship between elements also presents challenge in interpreting whether terms recited in claim language has the same meaning through out the entire claim language of a claim. For example, it is not clear whether "first data" recited in claim 97 on pg. 15 (line 6) is the same as "first data" recited in claim 97 pg. 16 (line 8). Furthermore, if it is not the same, it is not clear to which "first data" does "the first data" recited on pg. 16 (line 9) refers. For purposes of further examination "first data" recited on pg. 15, line 6 is treated as not corresponding to "first data" cited on pg. 16, line 8 and that "the first data" cited on pg. 16, line 9 corresponds to "first data" cited on pg. 16, line 8. However, the claim should be amended in order to leave no ambiguity to interpretations.

Summarizing, it is not clear which limitations in claims 2, 9 and 88-104 applicant attempts to seek a patent for and as a result metes and bounds of claimed invention cannot be determined.

18. The phrase: "it generates the first data from the second encrypted data including by decrypting the second encrypted data using the second secret value" in claim 88 is not understood.

19. Claim 90 recites circuitry that "in the first mode ... forwards, from the at least one serial link to the at least one additional serial link, multiply encrypted data received for decryption by the receiver in accordance with the first content protection protocol using the secret value, and in the second mode ... forwards the encrypted data to the at least one additional serial link for decryption by the receiver in accordance with the second content protection protocol using the third secret value". It is not clear whether the underlined limitations are directed towards the receiver or to the circuitry.

20. Claims 99-100 recites "a procedure for supplying a receiver key to the receiver". However, the procedure is not disclosed. Since in the art of record receivers use keys, the keys are inherently supplied to the receivers and the examiner considers that supplying the keys to the receivers reads on procedures for supplying a receiver keys.

21. The limitations of originally dependent on claim 4, claim 5 as amended should further limit the new claim 88. However, claim 5 appears to repeat the limitations of claim 88. Claim 88 reciting that "the external agent is configured to respond to a ticket request from one of the repeater and the receiver by determining or obtaining a determination as to whether to grant the request, and to send signals to the repeater and the receiver when coupled thereto in response to each granted ticket

request to enable the repeater and the receiver to operate respectively in an encryption mode and the decryption mode, wherein the signals include at least one of the secret value" and 5 recites: "wherein the repeater is configured to send a second ticket request to the external agent when the repeater is coupled to the external agent, and the external agent is configured to respond to the second ticket request by determining or obtaining a determination as to whether to grant the second ticket request, and sending second signals to the content source and the repeater in response to each granted second ticket request, wherein the second signals include at least one of the second secret value, an encrypted version of the second secret value, and data enabling the content source and the repeater to obtain the second secret value". As a result, it is not clear whether claim each requests requested in claim 5 and 88 should be considered as the same signals, whether they suggest that the external agent is contacted more than once by a repeater, or whether some other interpretation should be implemented.

22. Following lack antecedent basis:

- Claim 99: "the pseudo-random value"
- Claim 88: "the repeater",
- Claim 91: "the external controller".

Claim Rejections - 35 USC § 102

23. Claims 79-84, 99-102 are rejected under 35 U.S.C. 102(b) as being anticipated by *Menezes (Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237).*

Menezes teach providing a receiver key to the receiver (E(k)), providing a transmitter key to the transmitter (E(k)), operating the transmitter and the receiver to perform a challenge-response procedure (authentication using random numbers) to determine whether at least one of the transmitter key and the receiver key satisfies the predetermined criterion, wherein the operating step includes operating the receiver to encrypt first data in accordance with the protocol using the receiver key to generate an authentication message and sending the authentication message to the transmitter (A->B: Ek(rA, rB, B*)) operating the transmitter to perform a predetermined mathematical function on the authentication message to generate a result, to encrypt the result using the transmitter key to generate an encrypted result and sending the encrypted result to the receiver (A<-B: Ek(rB, rA)), and operating the receiver to generate a decrypted result by decrypting the encrypted result using the receiver key and determining from the decrypted result whether said at least one of the transmitter key and the receiver key satisfies the predetermine criterion (upon decrypting, A checks that the random number matches the one used earlier) (Menezes, 10.16 Remark section, in particular “3. mutual authentication , using random number”, pg. 402). The examiner points out that in order for the receiver to be enabled to the receiver key to decrypt data, the key must match the transmitter key, and the authentication process disclosed by *Menezes* validates that the receiver's key matches the sender's key.

24. As per claims 99-101, circuitries in network computer devices are inherent; in fact electronic circuitry is the main element that allows computer to perform operations such as the one discussed above.

25. As per claim 102 any data (rA) reads on key material since it is encrypted by Ek and sent to the receiver, which is consistent with applicant's clarification of the term: "key material" ("data for use by at least one of a transmitter and a receiver in an encryption and/or decryption process", applicant's remarks, pg. 21 paragraph 4).

Claim Rejections - 35 USC § 103

26. Claims 71-72 and 85 are rejected under 35 U.S.C. 103(a) as unpatentable over *Menezes (Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237).*

Menezes discloses the receiver configured o implement a content protection protocol, e.g. operating the receiver to generate the authentication message using a pseudo-random value (A->B: Ek(rA, rB, B*)) as disclosed above.

27. Although, *Menezes* does not explicitly disclose that the pseudo-random value is generated by a receiver. However, the limitation is at least implicit. There are only two communicating entities disclosed by *Menezes* and even if the receiver could receive a pseudo-random value from another (not disclosed device) it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to

configure the receiver to generate the pseudo-random value given the benefit of security (the value would be known only to the receiver) and efficiency.

28. Similarly implicit would have been configuring the receiver to treat the receiver key as an invalid key unless the decrypted result satisfies the predetermined criterion. As discussed above, the receiver key must match the transmitter key in order for the to successful data decryption.

29. Claims 13-14, 17, 20, 22, 25-26, 32-34, 54, 56 and 89-98 are rejected under 35 U.S.C. 103(a) as unpatentable over *Pfleeger (Charles P. Pfleeger, "Security in computing", 2nd edition, 1996, ISBN: 0133374866).*

A typical network environment inherently comprises a transmitter and a receiver coupled with a link configured to operate in a pass-through mode and non-decrypting mode in response to control signals *(e.g. Stallings, Fig. 1.2 pg. 6).*

30. *Pfleeger* discloses the concept of information security and discloses an enhancement to the typical network configuration with the transmitter and the receiver configured to implement a content protection protocol.

In *Pfleeger* the transmitter is extended to be operable in the encryption mode in which it generates encrypted data using a secret value (a key) and transmitting the encrypting data to the receiver, and extend the receiver to be operable in a decryption mode in which it generates decrypted data by decrypting the encrypted data using the secret value *(Pfleeger, Fig. 3-10, pg. 101).* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to extend a transmitter and a receiver of the typical network environment as taught by

Pfleeger. In particular it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to extend the transmitter to be operable in the encryption mode in which it generates encrypted data using a secret value and transmitting the encrypting data to the receiver, and to extend the receiver to be operable in a decryption mode in which it generates decrypted data by decrypting the encrypted data using the secret value. One of ordinary skill in the art would have been motivated to perform such a modification in order to provide ability to extend the typical a transmitter and a receiver secure to be operable to establish a secure communication channel.

31. Furthermore, in most common network environments an origin and a destination of data are connected using multiple computing devices (repeaters/routers) as disclosed by *Pfleeger* discloses of a repeater and a receiver connected through multiple repeaters *(pg. 386-37, Inter-Networks section).* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use multiple repeaters to connect a transmitter and a receiver given the benefit of an ability to connect two distant parties exchanging data while providing increased reliability *(Advantage of Computing Networks section, pg. 389).*

32. As discussed above it would have been obvious to utilize repeaters in order to connect two remote communicating parties. However, expanding on the advantages of connecting remote entities *Pfleeger* stresses the need to consider additional security measures, especially since in connecting remote transmitters and receivers additional intermediates are present *(Advantages of Computing Networks, pg. 389).*

As a solution to some of the security threats *Pfleeger* offers a link encryption involving a transmitter, a repeater and a receiver, wherein the transmitter and the repeater are configured to implement a content protection protocol, and the repeater and the receiver are configured to implement a second content protection protocol; a first link between the transmitter and the repeater, and second link between the repeater and the receiver, wherein the transmitter is configured to generate encrypted data by encrypting first data using a secret value and transmit the encrypted data over the first link to the repeater, the repeater is configured to generate decrypted data including by decrypting the encrypted data using the secret value, to generate re-encrypted data including by encrypting the decrypted data using a second secret value, and to transmit the re-encrypted data over the second link, and the receiver is configured to generate additional decrypted data by decrypting the re-encrypted data using the second secret value *(Link Encryption section, pg. 406)*. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement a link encryption. One of ordinary skill in the art would have been motivated to perform such a modification in order to provide communication security to address transmission line vulnerability. Implementation of link encryption would essentially result in essentially the repeater forwarding encrypted data received from the at least one link, and generating by the receiver encrypted data by decrypting the encrypted data using a secret value in accordance with a first content protection protocol.

33. On pg. 131-134 *(Symmetric Key Exchange with Server and Asymmetric Key Exchange with Server) Pfleeger* introduces an external agent *(a central key distribution service)* configured to be coupled to the receiver *(Renee)* and to the sender *(Pable)*, wherein at least one of the receiver and the transmitter is configured to send a ticket request to the external agent when coupled to the external agent, and the external agent is configured to respond to the request by determining or obtaining a determination as to whether to grant the request, and sending at least one signal to one of the transmitter and the receiver in response to each granted request, wherein the at least one signal is indicative of data that determines a pre-encrypted version of the key and data enabling the receiver to decrypt the pre-encrypted version of the key *(K[pr])*.

    It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the external agent in transmitter and receiver to distribute encryption keys as taught by *Pfleeger* given the benefit of flexible key distribution.

34. Extending external agent to communicate with multiple network devices would have been implicit given the benefit of scalability.

    Establishing a secure data exchange between a repeater and a receiver involving an external agent as disclosed by *Pfleeger* on page 131-134 would result in generating encrypted data by the repeater by performing a translation operation on multiply encrypted data received from the at least one link, wherein the translation operation would include decryption of the multiply encrypted data using a second secret value in accordance with a second content protection, forwarding by the repeater the encrypted data to the at least one additional link, and generating by the receiver decrypted data by decrypting the encrypted data in accordance with the second content protection protocol using a third secret value.

35. As per claims 93-94 the examiner treats a request for a secret value (a key) to the external agent (as disclosed above) as indicating capability of the receiver (e.g. an indication of the receiver to be able to receive data over the communication link from a sender) and the signal from the external agent as indicating capability of the receiver (e.g. capable to decrypt data).

36. Furthermore, as per claims 95-96, in order to receive a secret key that could be used in communication with the receiver the request must include the identity of the receiver that will be resolved into the communication key which can assert unprotected digital data at an output of the receiver (e.g. the receiver is capable to decrypt data) and assert digital data protected by a content protection protocol at an output of the receiver (can encrypt data).

37. The examiner treats the repeater recited in claim 92 as a part of the external agent (also recited in claim 92) that relates to one of the chain of devices (repeater/router disclosed by Pfleeger) that decrypt and re-encrypt data.

38. As per claim 89 *Pfleeger* does not explicitly disclose that encryption and decryption of data is accomplished with using the sequence of secret values the limitation, if not inherent, is at least implicit. Computers use 0 and 1 values and *Pfleeger* discloses that encryption/decryption keys use sequence of secret values *(e.g. 56bits, 128 bits etc. Pfleeger pg. 113).*

39. Furthermore, even if *Pfleeger* did not included using sequence of secret values in encryption/decryption process, including sequence of secret values in communication using encryption/decryption process is old and well-known (e.g. U.S. Patent No. 5412730 or rolling code encryption/decryption). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include sequence of secret values in encryption/decryption process given the benefit of increased security.

40. As per claim 97, *Pfleeger* does not disclose that the at least one signal is indicative of second data, wherein the second data includes a code value that identifies the secret key without revealing the secret key, and the secret key cannot be derived from the second data. However, Official Notice is taken that it is old and well-known practice to include indication of a second data without revealing the secret key, and the secret key cannot be derived from the second data (e.g. data identifying a key in systems utilizing a plurality of keys) given the benefit of increased complexity of braking encryption.

41. Claims 77 and 86-87 are rejected under 35 U.S.C. 103(a) as unpatentable over *Menezes (Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237)* in view of *Pfleeger (Charles P. Pfleeger, "Security in computing", 2nd edition, 1996, ISBN: 0133374866).* *Menezes* disclosure where two communicating entities perform a challenge-response using keys have been discussed above.

42. *Menezes* does not disclose coupling an external agent to the receiver and sending from an external agent to the receiver at least one of the receiver key, an encrypted version of the receiver key, and data enabling the receiver to obtain the receiver key.

43. *Pfleeger* discloses an external agent providing the key to communicating parties *(Pfleeger, pg. 131-134).* It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to couple an external agent to communicating parties sending to the receiver at least one of the receiver key, an encrypted version of the receiver key, and data enabling the receiver to obtain the receiver key given the benefit of secure key distribution.

44. Claims 5, 8 and 88 are rejected under 35 U.S.C. 103(a) as unpatentable over *Pfleeger (Charles P. Pfleeger, "Security in computing", 2nd edition, 1996, ISBN: 0133374866)* in view of *Davis (U.S. Patent No. 5805706).*

Pfleeger discloses a system implementing chain of communicating devices connected by communication links; the devices encrypting, decrypting and re-encrypting data with cooperation of an external agent using symmetric content protection protocol as discussed above. The examiner considers a content source and a repeater as one of these devices.

45. Although as discussed above, *Pfleeger* disclose devices implementing a decryption process (using circuitry to decrypt encrypted data) and an encryption process (re-encrypt data), *Pfeeger* does not explicitly disclose that a device (a repeater) comprises a first circuitry to generate the encrypted data and a second circuitry to decrypt data.

Davis discloses implementation of a secure system that includes decryption circuitry and encryption circuitry (e.g. Fig. 2 A and B). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a first circuitry to generate the encrypted data and a second circuitry to decrypt data as disclosed by Davis to provide efficiency and security into a decryption and a re-encryption process disclosed by *Pfleeger*.

46. The limitations of claim 5 are implicit. It would have been clear to one of ordinary skill in the art that devices disclosed by *Pfleeger* are devices for a multiple use (devices are used in communication multiple times) and that repeating the communication using the repeater and the external agent would result in a plurality of signals sent from the external agent to the repeater.

47. Claims 6-7 and 27-30 are rejected under 35 U.S.C. 103(a) as unpatentable over *Pfleeger (Charles P. Pfleeger, "Security in computing", 2nd edition, 1996, ISBN: 0133374866)* in view of *Davis (U.S. Patent No. 5805706)* and further in view of*Graunke (U.S. Pub. No. 20030005285).*

Pfleeger in view of *Davis* has been discussed above.

48. *Pfleeger* in view of *Davis* does not teach that the content protection protocols include AES and HDCP protocol.

Graunke teaches AES and HDCP protocol *[6 and 24]*.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use AES and HDCP protocols as taught by *Graunke*. One of ordinary skill in the art would have been motivated to perform such a modification given benefit of a proven common block cipher as well as extended data protection of content such as music by preventing unauthorized reproduction of the content.

49. AES 128 is one of the types of AES protocol and it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use such a protocol in order to encrypt/decrypt data (see NIST, for example).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: Walker (U.S. Patent No. 4991208).

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100